# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## 0. TRAZABILIDAD Y DISTRIBUCIÓN DEL DOCUMENTO.

| TABLA DE REVISIONES | | |
|---|---|---|
| **REVISIÓN** | **FECHA** | **MOTIVO DE LA REVISIÓN** |
| **01** | 01/04/2026 | Emisión Inicial. |
| | | |
| | | |
| | | |
| | | |

| DOCUMENTO PREPARADO Y REVISADO | | |
|---|---|---|
| **FIRMA** | **FECHA** | **PERSONA - CARGO** |
| Jofre Milá | 01/04/2026 | Jofre Milá<br>**Resp. Seguridad** |

| APROBACIÓN DOCUMENTO | | |
|---|---|---|
| **FIRMA** | **FECHA** | **PERSONA - CARGO** |
| Jordi Ribalta | 01/04/2026 | Jordi Ribalta<br>**CEO** |

El personal relacionado a continuación está autorizado para acceder al presente documento:

| | |
|---|---|
| **Responsable:** | **Responsable SI.** |
| **Lista de personal autorizado a acceder al documento:** | Todo el personal de la Entidad. |

## 1. OBJETO.

El objeto de la presente Política de Seguridad de la Información es determinar el alcance y estructura del sistema de Información (SI) implantado en **KAWARU CONSULTING**, en base a las directrices estipuladas en el Esquema Nacional de Seguridad, RD 311/2022, así como en la Norma UNE-EN ISO 27001:2023.

**KAWARU CONSULTING** depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada a los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuidad de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implican que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

**KAWARU CONSULTING** debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC.

**KAWARU CONSULTING** debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del Real Decreto 311/2022, de 4 de mayo, por el que se regula el Esquema Nacional de Seguridad en adelante (ENS)

## 2. ALCANCE.

El Alcance del Sistema de Seguridad de la Información de KAWARU CONSULTING es el siguiente:

***"Los Sistemas de Información que dan soporte a la prestación de los servicios de Consultoría Estratégica en el ámbito de la Innovación Tecnológica, tales como Desarrollo de Estrategias de Innovación, Implementación de Tecnologías Emergentes, así como el Diseño y Gestión de Proyectos, tanto para AA.PP como para entidades privadas."***

## 3. MISIÓN Y OBJETIVOS.

**KAWARU CONSULTING** unifica las perspectivas legal y tecnológica para ofrecer a sus clientes una solución integral a sus necesidades relacionadas con la prestación de servicios de Consultoría Estratégica para la realización de proyectos integrales en el ámbito de la Innovación Tecnológica, para el sector Público y Privado, y resto de servicios descritos en el Alcance.

**KAWARU CONSULTING** basa su actividad en el tratamiento de diferentes tipos de datos e información, ello le permite ejecutar procesos básicos propios del negocio. Los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyen el activo principal de **KAWARU CONSULTING,** de tal manera que el daño o pérdida de estos inciden en la realización de sus operaciones, y pueden poner en peligro la continuidad de la Organización.

Todo ello a través de escenarios de innovación permanente, investigación y desarrollo como elementos clave, y una cultura totalmente orientada a la excelencia en el servicio y al establecimiento de un marco de relación con los clientes y colaboradores como socios de negocio.

Estas cuestiones se materializan con las aportaciones de un amplio equipo de personas formadas, certificadas y en permanente actualización de conocimientos, así como en métodos y prácticas.

La excelencia en la ejecución, la fidelidad en el marco de relaciones y la empatía hacia el cliente y entre compañeros actúan como valores y principios básicos que rigen nuestra actuación.

En el ámbito concreto de la seguridad, el SI corporativo pretende lograr alcanzar **los siguientes objetivos:**

- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SI protegiendo la información interna y relacionada con la prestación de los servicios, considerando las dimensiones de:
  - Confidencialidad para asegurar que la información solo sea accedida por aquellos que cuenten con la autorización respectiva. Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
  - Integridad para preservar la veracidad y completitud de la información y los métodos de procesamiento. Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
  - Disponibilidad para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera. La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
  - Trazabilidad: Para asegurar que queda constancia fehaciente del uso del servicio y del acceso a los datos, es decir, que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.

- Autenticidad: Para asegurar que quien accede al servicio es realmente quien se cree y garantizar la fuente de la que proceden los datos. Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a duda.

- Demostrar liderazgo por parte de la dirección, dotando de recursos al SI y asegurando que la política y los objetivos de seguridad que se establezcan sean compatibles con la estrategia de la organización.
- Gestionar la implementación del SI de manera que proporcione ventajas competitivas en relación con otros agentes del sector, aprovechando la inercia que puede otorgar la gestión adecuada de la seguridad.
- Apostar por la **mejora continua**, y la implementación de medidas de seguridad eficaces y eficientes.
- Establecer anualmente objetivos, relacionados con ámbitos específicos de seguridad alineados con las normas de referencia del SI, ENS e ISO 27001.
- Cumplir con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad, alineando dichos requisitos con la privacidad y la seguridad de la información corporativa.
- Sensibilizar y concienciar de manera estable y permanente a todo el personal de la organización en cuanto a la seguridad de la información.
- Fomentar y mantener el buen nombre de la organización en relación con los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, mantenimiento la imagen y reputación.

## 4. PRINCIPIOS.

La política de seguridad de la información de **KAWARU CONSULTING** se desarrolla de acuerdo con los siguientes principios:

- **Principio de confidencialidad**: se deberá garantizar que la información sea accesible únicamente para aquellas personas expresamente autorizadas para ello.
- **Principio de integridad**: se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
- **Principio de disponibilidad**: se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.
- **Principio de gestión del riesgo:** Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.
- **Principio de mejora continua**: se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados para aumentar la capacidad de adaptación a la constante evolución del entorno.
- **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.

- **Principio de cumplimiento normativo**: todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.
- **Principio de prevención**: Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben: autorizar los sistemas antes de entrar en operación; evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria; solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

- **Principio de detección**: Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.
- **Principio de respuesta**: Los departamentos deben: establecer mecanismos para responder eficazmente a los incidentes de seguridad; designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos; establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- **Principio de recuperación**: Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

## 5. MARCO NORMATIVO.

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.
- Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

# 6. PRINCIPIOS BÁSICOS.

## 6.1 SEGURIDAD COMO PROCESO INTEGRAL.

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

## 6.2 GESTIÓN DE LA SEGURIDAD BASADA EN RIESGOS.

El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

## 6.3 PREVENCIÓN, DETECCIÓN, RESPUESTA Y CONSERVACIÓN.

### 6.3.1 Prevención.

**KAWARU CONSULTING** debe evitar, o al menos prevenir en la medida de lo posibles, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evolución de amenazas y riesgos.

Estos controles, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

### 6.3.2 Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

### 6.3.3 Respuesta.

**KAWARU CONSULTING**:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

### 6.3.4 Recuperación.

Para garantizar la disponibilidad de los servicios críticos, las distintas áreas de **KAWARU CONSULTING** deben desarrollar, cuando sea necesario, planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio de actividades de recuperación.

## 6.4 EXISTENCIA DE LINEAS DE DEFENSA.

El sistema de información dispondrá de una estrategia de protección constituida por diferentes capas, de forma que cuando una de las capas sea comprometida, permita desarrollar una acción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad del que el sistema sea comprometido en su conjunto, minimizando el impacto final sobre el mismo.

Existirán líneas de defensa constituidas tanto por medidas organizativas, físicas y lógicas.

## 6.5 VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA.

**KAWARU CONSULTING** llevará a cabo una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permite a **KAWARU CONSULTING** medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

**KAWARU CONSULTING** reevaluará y actualizará periódicamente las medidas de seguridad, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

## 6.6 DIFERENCIACIÓN DE RESPONSABILIDADES.

**KAWARU CONSULTING** tendrá en cuenta la diferenciación de responsabilidades en su sistema de información siempre que sea posible. El detalle de las atribuciones de cada responsable, los mecanismos de coordinación y la resolución de conflictos se detallarán a lo largo de la presente política de seguridad.

## 7. ORGANIZACIÓN DE LA SEGURIDAD.

La implantación de la Política de Seguridad en **KAWARU CONSULTING** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsables del Servicio

c) Responsables de la Información

d) Responsable de Seguridad de la Información

e) Responsable de Sistemas

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

### 7.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la Información es una responsabilidad organizativa que es compartida con la Dirección. En consecuencia, la Dirección de **KAWARU CONSULTING** promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vida definida y el palpable apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto por las figuras anteriormente mencionadas.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información;
    - Elaboración y actualización de planes de continuidad
    - Cumplimiento y difusión de las Políticas de Seguridad

### 7.2 RESPONSABLE DE LA INFORMACIÓN.

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos

- Determina los niveles de seguridad de la información.

### 7.3 RESPONSABLE DEL SERVICIO.

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.

- Determina los niveles de seguridad del servicio.

### 7.4 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN.

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo con los objetivos estratégicos de la Dirección.

El Responsable de Seguridad es el Punto de Contacto (PoC).

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de **KAWARU CONSULTING.**

- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:

    - La estrategia de seguridad de la información definida por el Comité de Seguridad.

    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de **KAWARU CONSULTING** y normativa de desarrollo.

- Supervisar (como responsable último) los incidentes de seguridad informática producidas en **KAWARU CONSULTING.**

- Difundir en **KAWARU CONSULTING** las normas y procedimientos contenidos en la Política de Seguridad de la Información de **KAWARU CONSULTING** y normativa de desarrollo, así como las funciones y obligaciones de todo **KAWARU CONSULTING** en materia de seguridad de la información.

- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.

- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de **KAWARU CONSULTING.**

### 7.5 RESPONSABLE DEL SISTEMA.

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad de **KAWARU CONSULTING,** de acuerdo con los objetivos estratégicos de **KAWARU CONSULTING.**

Las funciones del Responsable del Sistema de la Información son las siguientes:

- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de **KAWARU CONSULTING,** conforme a la estrategia de seguridad definida.

- Establecer la actuación de los Responsables Técnicos Informáticos, en los distintos entornos de seguridad que se designen.

- Garantizar la actualización del inventario de activos de Sistemas de Información de **KAWARU CONSULTING.**

- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.

- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en **KAWARU CONSULTING.**

- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.

- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.

- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

### 7.6 PROCEDIMIENTOS DE DESIGNACIÓN.

Mediante acta se designan las siguientes responsabilidades:

- **Responsable del Servicio**
- **Responsable de la Información**
- **Responsable de Seguridad**
- **Responsable del Sistema**

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Seguridad.

### 7.7 RESOLUCIÓN DE CONFLICTOS.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad, elevándose para su resolución a la Dirección en caso de no llegar a un acuerdo.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

## 8. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

## 9. DATOS DE CARÁCTER PERSONAL.

**KAWARU CONSULTING** trata datos de carácter personal.

Todos los sistemas de información de **KAWARU CONSULTING** se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado 5. Marco Normativo, de la presente Política de Seguridad de la Información.

## 10. GESTIÓN DE RIESGOS.

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

## 11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Esta Política de Seguridad de seguridad se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad, de acuerdo al marco organizativo definido en el **apartado 7 de esta Política.**
- Análisis y gestión de los riesgos, de acuerdo con lo previsto en el procedimiento **KAW-GR-01 Metodología de Análisis de Riesgos**
- Gestión de personal, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-22 Gestión de personal.**
- Profesionalidad, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-22 Gestion de personal.**
- Autorización y control de los accesos, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-05 Control de acceso.**
- Protección de las instalaciones, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-09 Seguridad Física.**
- Adquisición de productos, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-16 Procesos de Autorización y KAW-PSSI-07 Gestión de Proveedores.**
- Mínimo privilegio, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-05 Control de acceso.**

- Integridad y actualización del sistema, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-06 Seguridad Lógica.**
- Protección de la información almacenada y en tránsito, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-06 Seguridad Lógica.**
- Prevención ante otros sistemas de información interconectados, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-23 Protección de las comunicaciones.**
- Registro de actividad, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-05 Control de acceso.**
- Incidentes de seguridad, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-10 Gestión de Incidentes de Seguridad.**
- Continuidad de la actividad, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-08 Continuidad del Negocio.**
- Mejora continua del proceso de seguridad, de acuerdo con lo previsto en el procedimiento **KAW-PSSI-08 Continuidad del Negocio.**

## 12. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN.

Las directrices para la estructuración, gestión y acceso a la documentación de seguridad del sistema de Gestión Seguridad de la Información de **KAWARU CONSULTING,** se definen en el procedimiento **KAW-PSSI-01 Control de la Documentación y los Registros.**

Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por la Dirección de **KAWARU CONSULTING** a propuesta del Comité de Seguridad.

- Segundo nivel: la normativa de seguridad de la información aprobada por la Dirección de **KAWARU CONSULTING.** En ella se establecerán unas normas de uso aceptable de los sistemas de información.

- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Comité de Seguridad.

- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Estos documentos han de ser aprobados por el Comité de Seguridad.

Los documentos que integran el SGSI se encuentran, en soporte digital, a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo. Estará disponible para su consulta, sin posibilidad de modificación.

## 13. CALIFICACIÓN DE LA INFORMACIÓN.

Para calificar la información **KAWARU CONSULTING** atenderá a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.

Tanto el responsable de cada información manejada por el sistema como los criterios de calificación de la información, que determinarán el nivel de seguridad requerido, se establecen en el procedimiento **KAW-PSSI-11 Calificación y Etiquetado de la Información**

## 14. OBLIGACIONES DEL PERSONAL.

Todos y cada uno de los usuarios de los sistemas de información de **KAWARU CONSULTING** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de **KAWARU CONSULTING** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de **KAWARU CONSULTING** recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **KAWARU CONSULTING,** en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

## 15. INCLUMPLIMIENTO.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

## 16. DOCUMENTACIÓN RELACIONADA.

- KAW-ENS-04 Asignación de Roles y Responsabilidades para la Seguridad de la Información.
- Acta del Comité de Seguridad con los nombramientos asociados a cada uno de los Roles relativos a Seguridad de la Información.
- Instrucciones Técnicas CCN-STIC-Serie 800, emitidas por el CCN.
- RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.